& L10/#5 applied 12/15

Set Name side by side	Query	Hit Count	Set Name result set
	DB=USPT; PLUR=YES; OP=ADJ		
L10	L8 and (communicat$ with different with networks)	10	L10
L9	L8 and (communicat$ with networks)	37	L9
L8	L1 and ((compar$ with IP with address$) and ((substitute$ or replace$) with address$))	41	L8
L7	L6 and (communicat$ with networks)	151	L7
L6	L1 and ((compar$ with address$) and ((substitute$ or replace$) with address$))	256	L6
L5	L2 and (internet same (intranet or lan))	5	L5
L4	L1 and ((compar$ with address$) same (substitute$ with address$) and (internet and (intranet or lan)))	5	L4
L3	L1 and ((compar$ with address$) same (substitute$ with address$) same (internet and (intranet or lan)))	0	L3
L2	L1 and ((compar$ with address$) same (substitute$ with address$))	11	L2
L1	((709/$)!.CCLS.)	17420	L1

END OF SEARCH HISTORY

(1) commun. bet. diff networks

(2) replac IP address.

(3) compar IP addr.

(4) 709

WEST

Generate Collection | Print

Search Results - Record(s) 1 through 10 of 10 returned.

☐ 1. Document ID: US 6618366 B1

L10: Entry 1 of 10 File: USPT Sep 9, 2003

DOCUMENT-IDENTIFIER: US 6618366 B1
TITLE: Integrated information communication system

Brief Summary Text (8):
However, with the Internet, the path control is restricted by IP, so that one cannot tell whether the other party with which communication is being made is the authorized party, and the system is such that the communication path is not administrated in an integrated manner, meaning that there are problems regarding security in that information may be eavesdropped. Also, in reality, addresses within the LANs are being separately decided by the LAN users, so there is the necessity to replace the LAN user addresses when connecting the LAN to the Internet. Also, communication quality such as communication speed and communication error rate for the trunk lines making up the Internet communication path differ from one line to another for each LAN, and are practically non-uniform. Also, there are problems such as an attempt to send a 10 Mbps TV signal for video-conferencing not achieving the desired communication speed. Further, there is no administrator for performing maintenance of the network such as in the case of failure, or for integrating the overall network for future planning for the network and so forth. Also, with LAN networks and the Internet, the terminals are personal computers (computers), and it has been difficult to use telephones, FAX and CATV in an integrated manner therein.

Detailed Description Text (46):
Now, description of the operation of a virtual dedicated line connection according to the present invention will be made with reference to FIG. 20. Here, the virtual dedicated line connection refers to communication wherein ICS user packets are transferred in a fixed manner to a receiving ICS network address already registered in the conversion table, regardless of the ICS user address within the user control field of the ICS user packet, in which the format taken is one-on-one or one-on-N. While the components of FIG. 20 are the same as those of Embodiment-1 shown in FIGS. 14 and 15, what is different is the contents of registration in the conversion table. In the conversion table of the access control apparatus, the receiving ICS network address is determined from the transmitting ICS network address in a fixed manner, so that either the sender ICS user address (intra-corporation), the sender ICS user address (inter-corporation) and the receiver ICS user address are either not registered, or ignored if registered.

Detailed Description Text (62):
Appropriated to the access control apparatus 1010-5 shown in FIG. 27 are ICS network addresses "7711" and "7722", serving as connection points (ICS logic terminals) for corporations X and A which are the users of the ICS 905. Also appropriated to the access control apparatus 1010-7 are ICS network addresses "7733" and "7744", serving as connection points for corporations W and C, similarly. In FIG. 28, appropriated to the access control apparatus 1010-6 are ICS network addresses "9922" and "9933", serving as connection points for corporations Y and B, and similarly appropriated to the access control apparatus 1010-8 are ICS network addresses "9944" and "9955", serving as connection points for corporations Z and D. Here, in the ATM network embodiment, the corporations X, Y and so forth, which are given as examples of users, may be differing locations within a single corporation which performs intra-corporation communication, or may be different corporations which perform

inter-corporation communication.

Detailed Description Text (143):
Appropriated to the access control apparatus 1010-5 are ICS network addresses "7711" and "7722", serving as connection points (ICS logic terminals) for the corporations X and A which are the users of the ICS 925. Also appropriated to the access control apparatus 1010-7 are ICS network addresses "7733" and "7744", serving as connection points for the corporations W and C, similarly. Appropriated to the access control apparatus 1010-6 are ICS network addresses "9922" and "9933", serving as connection points for the corporations Y and B, and similarly appropriated to the access control apparatus 1010-8 are ICS network addresses "9944" and "9955", serving as connection points for the corporations Z and D. Here, in the embodiment shown in FIGS. 39 and 40, etc., the corporations X, Y and so forth, which are given as examples of users, may be differing locations within a single corporation which performs the intra-corporation communication, or may be different corporations which perform the inter-corporation communication.

Detailed Description Text (268):
Another version will be described with reference to FIG. 66. In FIG. 61, the satellite transmission corporation 16300-1, the IP terminal 16310-1 of the satellite transmission corporation, the database 16320-1 of the satellite transmission corporation, and satellite transmission equipment 16330-1 of the satellite transmission corporation are each within the ICS 16000-1, the IP terminal 16310-1 being provided with an ICS special number "4300". As compared to this, in the example shown in FIG. 66, the satellite transmission corporation 16300-2, the IP terminal 16310-2 of the satellite transmission corporation, the database 16320-2 of the satellite transmission corporation, and the satellite transmission equipment 16330-2 of the satellite transmission corporation are each outside of the ICS 16000-2, the IP terminal 16310-2 being provided with an ICS user address "3900". The data providing corporation 16200-1 and users 16500-1, 16510-1, 16520-1 are capable of sending and receiving of IP packets completely regardless of whether the other party has an ICS user address or an ICS special number, so sending and receiving of IP frames can be performed in combination with satellite communication with the example in FIG. 66 just as with that in FIG. 61.

Detailed Description Text (278):
Another version will be described with reference to FIG. 66. In FIG. 61, the satellite transmission corporation 16300-1, the IP terminal 16310-1 of the satellite transmission corporation, the database 16320-1 of the satellite transmission corporation, and the satellite transmission equipment 16330-1 of the satellite transmission corporation are each within the ICS 16000-1, the IP terminal 16310-1 being provided with an ICS special number "4300". As compared to this, in the example shown in FIG. 66, the satellite transmission corporation 163002, the IP terminal 16310-2 of the satellite transmission corporation, the database 16320-2 of the satellite transmission corporation, and the satellite transmission equipment 16330-2 of the satellite transmission corporation are each outside of the ICS 16000-2, the IP terminal 16310-2 being provided with an ICS user address "3900".

Detailed Description Text (287):
Another version will be described with reference to FIG. 66. In FIG. 61, the satellite transmission corporation 16300-1, the IP terminal 16310-1 of the satellite transmission corporation, the database 16320-1 of the satellite transmission corporation, and the satellite transmission equipment 16330-1 of the satellite transmission corporation are each within the ICS 16000-1, the IP terminal 16310-1 being provided with an ICS special number "4300". As compared to this, in the example shown in FIG. 66, the satellite transmission corporation 16300-2, the IP terminal 16310-2 of the satellite transmission corporation, the database 16320-2 of the satellite transmission corporation, and the satellite transmission equipment 16330-2 of the satellite transmission corporation are each outside of the ICS 16000-2, the IP terminal 16310-2 being provided with an ICS user address "3900".

Detailed Description Text (296):
Another version will be described with reference to FIG. 66. In FIG. 61, the satellite transmission corporation 16300-1, the IP terminal 16310-1 of the satellite transmission corporation, the database 16320-1 of the satellite transmission

corporation, and the satellite transmission equipment 16330-1 of the satellite transmission corporation are each within the ICS 16000-1, the IP terminal 16310-1 being provided with an ICS special number "4300". As compared to this, in the example shown in FIG. 66, the satellite transmission corporation 163002, the IP terminal 16310-2 of the satellite transmission corporation, the database 16320-2 of the satellite transmission corporation, and the satellite transmission equipment 16330-2 of the satellite transmission corporation are each outside of the ICS 16000-2, the IP terminal 16310-2 being provided with an ICS user address "3900".

Detailed Description Text (308):
Another version will be described with reference to FIG. 75. In FIG. 73, the satellite transmission corporation 16300-3, the IP terminal 16310-3 of the satellite transmission corporation, the database 16320-1 of the satellite transmission corporation, and the satellite transmission equipment 16330-3 of the satellite transmission corporation are each inside the ICS 16000-3, the IP terminal 16310-3 being provided with an ICS special number "4300". As compared to this, in the example shown in FIG. 75, the satellite transmission corporation 163004, the IP terminal 16310-4 of the satellite transmission corporation, the database 16320-2 of the satellite transmission corporation, and the satellite transmission equipment 16330-4 of the satellite transmission corporation are each outside of the ICS 16000-3, the IP terminal 163104 being provided with an ICS user address "3900".

Current US Cross Reference Classification (8):
709/203

Current US Cross Reference Classification (9):
709/220

Current US Cross Reference Classification (10):
709/230

Current US Cross Reference Classification (11):
709/238

Current US Cross Reference Classification (12):
709/249

☐ 2. Document ID: US 6427170 B1

L10: Entry 2 of 10 File: USPT Jul 30, 2002

DOCUMENT-IDENTIFIER: US 6427170 B1
TITLE: Integrated IP address management

Brief Summary Text (5):
Data communications networks are widespread and there are many different types of networks, including LANs (Local Area Networks), MANs (Metropolitan Area Networks), and WANs (Wide Area Networks). They are used for providing numerous services, both for companies and for individuals. They provide a powerful communication mechanism and allow access to various kinds of remote information. Two or more networks connected together form an internetwork (or internet). The "Internet" is a worldwide internet widely used to connect universities, government offices, companies, and private individuals. Every host (or end-user's machine running user applications) and router interface on the Internet has an IP address, which encodes its network number and host number. The combination is unique and no two machines have the same IP address. IP addresses are typically 32 bits long and are used in the source address and destination address fields of IP packets. The Source Address is the

ultimate source of the IP packet; the Destination Address is the ultimate destination of the IP packet.

Brief Summary Text (18):
Currently, the only solution for Telcos and ISPs to manage the shortage of IP addresses is to configure a Network Access Server (NAS) in each PoP (point of presence) so as to implement DHCP-like functionality with IP address pools so as to dynamically allocate IP addresses. That is, the NAS hands out IP addresses to users (end-users of the Telco or ISP) when the users log-in, and revokes them when the users log-out, making those IP addresses available to other users. Such mechanisms make it impossible to reliably (a) locate users by name; and (b) account for usage. A distributed DHCP server, for example, in a PoP, leases IP addresses from its IP address pool to be assigned to hosts on a temporary basis. This mechanism is more "granular" and addresses the problems stated above. These "dynamic" IP addresses are compared with "static" IP addresses that are practically permanently allocated and recorded, typically, in DNS servers.

Detailed Description Text (23):
When the local cache 6 receives the published events, it updates the IP address database and the user record database in the local cache 6. In accordance with a presently preferred embodiment, the local cache 6 receives the IP address allocation events and the IP address revoke events, and updates the contents of the IP address database (IP address table) and the user record database (user profile) based on the received events. For example, an entry is added to the IP address database when an IP address is reported by the IP address allocation event, and the entry is removed when the IP address is reported by the IP address revoke event. Fields in the user record database such as the IP address allocation field are checked and updated in accordance with the update/change in the IP address database. By checking and comparing the entry of the IP table and the corresponding IP address allocation field in the user table, errors, if any, in both tables are corrected and logged, in addition to updating the records in both tables.

Detailed Description Text (24):
The local cache 6 may further subscribe, through the adapter 16, to the accounting start events and update the contents of the IP address database based on the accounting start events. The local cache 6 may further subscribe to the accounting stop events, and further update the contents of the user record database based on the accounting start events and accounting stop events. For example, the expiry time of an IP address allocated will be replaced by the time the user logged out. However, it should be noted that the allocated IP addresses on the IP address database are revoked only when they are reported by the IP address revoke events published by the network controller 30, but not when reported by the accounting stop events published from the protocol gateway 4 in a PoP. This realizes that the IP address databases distributed among PoPs are centrally managed by the network controller 30.

Detailed Description Text (32):
The primary DNS server 12 may include a disk memory 46 from which the primary cache 44 obtains the data, and a secondary cache memory 48 that obtains its information from the primary cache 44. In order to back-up the information, the secondary cache memory 48 is preferably implemented by a different machine from that of the primary cache memory 44. When an IP address is reported by the accounting start event, each one of the DNS servers 12 and 14 adds an entry of the association for the IP address if the IP address is not already on the records. If the IP address already exists on the record and is associated with a different domain name, the existing domain name is replaced with a newly reported name, logging the error. If the IP address exists and is associated with the same domain name as the reported name, the DNS server may ignore that record (the record remains unchanged).

Detailed Description Text (55):
FIG. 10A illustrates one presently preferred embodiment of the IP address revoke operation. The network controller 30 implements a timer and associates the timer with the IP Address Table maintained in the Primary Mother Cache. When the timer expires (S184), the network controller 30 examines the IP address Table to identify IP addresses that may need to be revoked. The network controller 30 adds the expiry

time (seconds) allocated for the IP address (plus a configured grace time) to the time the IP address was allocated, and compares that time with the present time (S186). If the IP address has expired, the network controller 30 looks up the associated user record in the User Table to determine if the user has logged on or not (S188). If the user is not logging on, the network controller 30 then moves that IP address to a database for IP address revoke events (S190). In accordance with a presently preferred embodiment, this database may be a table of IP addresses that need to be revoked (IP Address Revoke Table). The network controller 30 also updates the correct offset in the IP Address Allocated field of the User Table to reflect that the IP address has been revoked and adjusts the same offset in the Session Information field to reflect that this session is now available (S192). Then, as shown in FIG. 10C, based on a timer, the network controller 30 periodically publishes the IP address revoke events through the IP Address Management Interface (S200).

Current US Original Classification (1):
709/226

Current US Cross Reference Classification (1):
709/228

☐ 3. Document ID: US 6397259 B1

L10: Entry 3 of 10 File: USPT May 28, 2002

DOCUMENT-IDENTIFIER: US 6397259 B1
TITLE: Method, system and apparatus for packet minimized communications

Detailed Description Text (99):
The thin protocols used between the wireless client 405 and the proxy server 180 are IP based. IP based protocols are widely used and enable the wireless client 405 to communicate with many different wireless networks. Furthermore, basing wireless client 405 and proxy server 180 processing resources on IP provides a layer of isolation and independence from the actual wireless network in use.

Detailed Description Text (447):
The ADDRESS start tag will be replaced with the appropriate tagTextSize, tagTextFont, etc. CML tags as necessary in order to represent the address section in a proportional, normal size, italic font.

Detailed Description Text (1084):
The wireless network interface 510 can determine if a packet can be compressed into this format by checking that the destination IP address is for the proxy server 180, that the protocol is UDP, and that the destination UDP port number is for the proxy server 180 service port. Determining that the destination IP address is for the proxy server 180 can be done by checking for a special value or comparing it with a value that has been registered with the wireless network interface 510 through a settings call. Since the packet itself will not go out onto the Internet 190, the address used to identify the proxy server 180 does not have to be a unique Internet IP address.

Current US Original Classification (1):
709/236

Current US Cross Reference Classification (1):
709/247

☐ 4. Document ID: US 6393487 B2

L10: Entry 4 of 10 File: USPT May 21, 2002

DOCUMENT-IDENTIFIER: US 6393487 B2
TITLE: Passing a communication control block to a local device such that a message is processed on the device

Brief Summary Text (11):
The above description of layered protocol processing is simplified, as college-level textbooks devoted primarily to this subject are available, such as Computer Networks, Third Edition (1996) by Andrew S. Tanenbaum, which is incorporated herein by reference. As defined in that book, a computer network is an interconnected collection of autonomous computers, such as internet and intranet systems, including local area networks (LANs), wide area networks (WANs), asynchronous transfer mode (ATM), ring or token ring, wired, wireless, satellite or other means for providing communication capability between separate processors. A computer is defined herein to include a device having both logic and memory functions for processing data, while computers or hosts connected to a network are said to be heterogeneous if they function according to different operating systems or communicate via different architectures.

Detailed Description Text (99):
When a frame is received by the INIC, it must verify it completely before it even determines whether it belongs to one of its TCBs or not. This includes all header validation (is it IP, IPV4 or V6, is the IP header checksum correct, is the TCP checksum correct, etc). Once this is done it must compare the source and destination IP address and the source and destination TCP port with those in each of its TCBs to determine if it is associated with one of its TCBs. This is an expensive process. To expedite this, we have added several features in hardware to assist us. The header is fully parsed by hardware and its type is summarized in a single status word. The checksum is also verified automatically in hardware, and a hash key is created out of the IP addresses and TCP ports to expedite TCB lookup. For full details on these and other hardware optimizations, refer to the INIC Hardware Specification sections (Heading 8).

Detailed Description Text (792):
The Map instruction is provided to allow replacement of instructions which have been stored in ROM and is implemented any time the "map enable" (MapEn) bit has been set and the content of the "map address" (MapAddr) field is non-zero. The instruction decoder forces a jump instruction with the Alu operation and destination fields set to pass the MapAddr field to the program control block.

Current US Original Classification (1):
709/238

Current US Cross Reference Classification (1):
709/230

☐ 5. Document ID: US 6377990 B1

L10: Entry 5 of 10 File: USPT Apr 23, 2002

DOCUMENT-IDENTIFIER: US 6377990 B1
TITLE: System for providing internet access from locations different from those for which the user's software was configured

Brief Summary Text (17):
The present invention is a method for operating a local area network having a server and a plurality of computers. The server includes an Internet gateway for directing messages to and from the Internet. Each computer in the network has a unique IP address and a unique network adapter address associated with that computer. Each computer determines the network adapter address associated with a target IP address by broadcasting an address resolution protocol (ARP) message on the local area network. The ARP includes the target IP address and the network adapter address and IP address of the computer broadcasting the ARP. The computer having the target IP address responds to an ARP by sending a response message that includes the network adapter address of the computer having the target IP address. In the present invention, the server stores information identifying IP addresses in a foreign class corresponding to computers not configured for connection to the local area network. The server responds to each ARP having a target IP address in the foreign class by returning the network adapter address of the server in the response message and assigning an IP address associated with the local area network to the IP address of the computer sending the ARP. The server translates each outbound message originating on the local area network for a destination address in the foreign class from an originating address for which one of the IP addresses associated with the local area network has been assigned. The translation consists of replacing the IP address of the computer originating the message with the corresponding IP address assigned to that computer. The translated message is then sent via the gateway. The sever also examines each inbound message received on the gateway for a destination IP address associated with the local area network to determine if the destination address is an IP address that has been assigned to an IP address in said foreign class. If such an assignment has been made, the server replaces the destination IP address in the message with the foreign IP address and sends the inbound message on the local area network.

Replaces
125-28 col 3

Detailed Description Text (8):
When a computer first attempts to contact another computer, it determines the Ethernet address that corresponds to the target IP address by sending an address resolution protocol (ARP) message containing its IP address, its Ethernet address, and the target IP address. All Ethernet adapters on the network unpack this message and pass on the message to the Ethernet drivers which compare the IP addresses associated with their Ethernet adapters to the target IP address. If an IP address matches, a return packet is sent to the sender giving the Ethernet address associated with the target IP address.

l24-35 col 4

Copies

Detailed Description Text (9):
Consider the case in which work-station 16 boots up and wishes to determine the address of the Ethernet adapter associated with gateway 11. Computer 16 has the IP address of the gateway stored in its network configuration data. To find the corresponding Ethernet address, work-station 16 broadcasts an ARP message on network 20. This message contains the IP address of work-station 16, the Ethernet address of work-station 16, and the IP address whose Ethernet address is being sought, i.e., the IP address associated with gateway 11. Each network adapter reads this message and the interface software compares the target IP address with that associated with the computer connected to the network card. If the IP addresses match, a reply message giving the Ethernet address of the network card is sent back to the requesting computer.

l 45-5 col 4

Copies

Detailed Description Text (14):
Basically, a server according to the present invention processes a message directed to a non-local IP address by translating the source IP address from the home IP address to the hotel IP address and then sending the message on the Internet. When the server receives a message from the Internet for a hotel IP address, the server replaces the destination address with the corresponding home IP address and places

replaces

33-43 col 5

the message on the local area network at the hotel. This protocol is sufficient to assure that messages are properly delivered without changing the IP address of the user's computer.

Detailed Description Text (20):
It should also be noted that the mobile computer user may also have an IP address stored for a DNS server that makes the translation from an ASCII address such as "compuserve.com" to the corresponding IP address on the Internet. Many local area networks utilize local servers for this process, and hence, the IP addresses will also be invalid on the hotel's network. These messages are easily detected since they are directed to a specific"port" on the invalid IP address. In the preferred embodiment of the present invention, the server treats all DNS messages as being directed to an invalid IP address and substitutes a valid DNS address associated with the local server.

Current US Original Classification (1):
709/225

Current US Cross Reference Classification (2):
709/220

Current US Cross Reference Classification (3):
709/242

CLAIMS:

1. A method for operating a local area network having a server and a plurality of computers including a first computer, said server including an Internet gateway, each computer in said local area network having a unique IP (Internet protocol) address and a unique network adapter address associated with that computer, each computer determining the network adapter address associated with a target IP address by broadcasting an address resolution packet (ARP) on said local area network, said ARP including at least said target IP address and said network adapter address and IP address of said computer broadcasting said ARP, said computer having said target IP address responding by sending a response message that includes said network adapter address of said computer having said target IP address, at least said first computer being connectable to a home network different from said local area network, said method comprising the steps of:

using a first IP address by said first computer when said first computer communicates using said home network;

storing information identifying IP addresses in a foreign class corresponding to computers not configured for connection to said local area network including storing said first IP address of said first computer;

sending a first communication from said first computer to said server;

causing said server to send a response to each ARP having a target IP address in said foreign class, said server returning said network adapter address of said server in said response message and assigning an IP address associated with said local area network to said IP address of said computer sending said ARP in said response including assigning by said server after receiving said first communication from said first computer a second IP address associated with said local area network to said first computer that is different from said first IP address of said first computer, said second IP address being assigned independently of program code provided with said first computer to obtain said second IP address;

causing said server to translate each outbound message originating on said local area network for a destination address in said foreign class from an originating address for which one of said address' associated with said local area network has been assigned, including a first outbound message, different from said first communication, sent to said server by said first computer using said first IP address, by replacing said first IP address of said computer originating said message with said corresponding second IP address assigned to that computer, said

first computer operating at all times independently of said second IP address when said first computer is connected to said local area network including when said first computer sends first outbound message to said server; and

sending said translated outbound messages via said gateway including using said second IP address to send said first outbound message from said server via said gateway.

7. A method for communicating using a global computer network, comprising:

establishing a first address associated with a computer that can be connected to a first network having a first server wherein, when said computer communicates to the global computer network using said first network, said computer uses said first address;

connecting said computer to a second network having a second server in which said first address is recognized by said second server as being different from computers that are part of said second network, said step of connecting including sending a first communication from said computer to said second server and associating a global computer network address to said computer by said second server independently of program code provided with said computer to obtain said global computer network address; and

providing a second communication, different from said first communication, between said computer and the global computer network, said providing step including providing said second communication from said computer to said second server using a second network address and providing said second communication to the global computer network by said second server using said global computer network address, said computer operating at all times independently of said global computer network address when said computer is connected to said second network and said second communication is provided independently of said computer using said global computer network address.

18. An apparatus for communicating using a global computer network in which a computer has two different addresses, comprising:

a computer having a first address associated with a first network wherein, when communicating to the global computer network using a first server on said first network, said computer uses said first address; and

a second network to which said computer is connected, said second network including a second server, said second server associating a global computer network address with said computer independently of program code provided with said computer to obtain said global computer network address;

wherein said computer, when sending each communication to the global computer network using said second server, sends said communication to said second server using a second network address, and said second server changes said second network address to said global computer network address in order to send each said communication to the global computer network, said computer operating at all times independently of said global computer network address when connected to said second server including when each said communication is sent to the global computer network.

DOCUMENT-IDENTIFIER: US 6334153 B1
TITLE: Passing a communication control block from host to a local device such that a message is processed on the device

Brief Summary Text (11):
The above description of layered protocol processing is simplified, as college-level textbooks devoted primarily to this subject are available, such as Computer Networks, Third Edition (1996) by Andrew S. Tanenbaum, which is incorporated herein by reference. As defined in that book, a computer network is an interconnected collection of autonomous computers, such as internet and intranet systems, including local area networks (LANs), wide area networks (WANs), asynchronous transfer mode (ATM), ring or token ring, wired, wireless, satellite or other means for providing communication capability between separate processors. A computer is defined herein to include a device having both logic and memory functions for processing data, while computers or hosts connected to a network are said to be heterogeneous if they function according to different operating systems or communicate via different architectures.

Detailed Description Text (99):
When a frame is received by the INIC, it must verify it completely before it even determines whether it belongs to one of its TCBs or not. This includes all header validation (is it IP, IPV4 or V6, is the IP header checksum correct, is the TCP checksum correct, etc). Once this is done it must compare the source and destination IP address and the source and destination TCP port with those in each of its TCBs to determine if it is associated with one of its TCBs. This is an expensive process. To expedite this, we have added several features in hardware to assist us. The header is fully parsed by hardware and its type is summarized in a single status word. The checksum is also verified automatically in hardware, and a hash key is created out of the IP addresses and TCP ports to expedite TCB lookup. For full details on these and other hardware optimizations, refer to the INIC Hardware Specification sections (Heading 8).

Detailed Description Text (766):
The Map instruction is provided to allow replacement of instructions which have been stored in ROM and is implemented any time the "map enable" (MapEn) bit has been set and the content of the "map address" (MapAddr) field is non-zero. The instruction decoder forces a jump instruction with the Alu operation and destination fields set to pass the MapAddr field to the program control block.

Current US Original Classification (1):
709/230

Current US Cross Reference Classification (1):
709/238

Current US Cross Reference Classification (2):
709/250

☐ 7. Document ID: US 6262976 B1

L10: Entry 7 of 10 File: USPT Jul 17, 2001

DOCUMENT-IDENTIFIER: US 6262976 B1
TITLE: System and method for network flow optimization using traffic classes

Brief Summary Text (4):
Modularized/layered solutions or "protocols" are known which permit computer systems to communicate, regardless of connection method or vendor-specific hardware implementation, or to permit different networks to communicate or be "internetworked." Known systems provide for connectivity in and among networks of computerized equipment, and address the problems associated with interconnectivity. Layering in known systems divides the task of interconnection and communication into pieces (layers), wherein each layer solves a piece of the problem or provides a particular function and is interfaced to adjacent layers. Each of the layers is responsible for providing a service to ensure that the communication is properly effected. Examples of some services provided by the various layers are error detection, error recovery, and routing among many communication paths. All the layers in conjunction present the overall communication protocol. It is generally well accepted in the art of internetworking that modularizing in layers with well defined functional interfaces, divides and effectively reduces the complexity of the connectivity problem and leads to a more flexible and extensible solution.

Brief Summary Text (7):
TCP/IP is a four layer protocol suite which facilitates the interconnection of two or more computer systems on the same or different networks. In certain networks, such as the Internet, TCP/IP is a requirement for interoperability. The four layers comprise two independent protocols: TCP which can be used to access applications on other systems within a single network; and IP which permits identification of source and destination addresses for communication between systems on different networks.

Detailed Description Text (28):
One spin-off of relative addressing is that the domain name space services are distributed across network routers to properly translate relative ON addresses between relatively positioned end stations. The relative destination address for a host within a remote domain would resolve through DNS to a different address from a host within the destination host's domain. Two hosts within the same destination domain, with different proximity to the destination host, would resolve to different addresses. The importance is that the relative addresses within the connecting fabric deliver data to the same destination host. Though relative addressing, the performance of forwarding will dramatically outweigh the overhead of fixed changes to (known) IP addresses by connecting network elements. The simplifications to the forwarding table lookups overshadow IP to relative address handling. Even inter-domain address conversion and network address translation to standard IP systems add insignificant performance costs to relative addressing compared to the performance increases of switching vs. routing for forwarding.

Detailed Description Text (31):
When data is being routed across network elements the address appearance will vary based on the connectivity of the two quantities. When two hosts on different networks are communicating through an adjoining router, the quantities appear as: 0.0.linknumber.hostnumber. Therefore the lookup for the router has been reduced to a direct index into an ordered array of quantities based on link number for this type of forwarding. This can be implemented in hardware as can the masking of the local IP address. Compatibility with standard IP on the end hosts is assured because to the two end hosts they appear on differing networks. End stations check the destination IP network address for a match with the source host's network to determine if it is a local address or not. If it is local, the hosts communicate together without a router. If the two addresses are different, the end stations send the IP data to their default router. This simplifies router lookup for this type of forwarding.

Detailed Description Text (275):
For Local Switch Network Data Structures; for Src and Dst NE's on the same network switch but different links communicating, the addresses look like:

Detailed Description Text (293):
With regard to Multiple Switch Network Data Structures, for Src and Dst NE's in the same network but different switches and links communicating, the addresses look like:

Detailed Description Text (414):
Fabric Domains or backbone networks provide inter-connections not between hosts but between domains. With Ordered Networking, substantially every data structure and algorithm previously explained applies directly to backbone inter-connections with a simple change of scale. In each of the previous discussions, the source and destination address pair represented a co-ordinate system for a local interior domain consisting of hosts. If the word host is replaced with domain, and each of the access fields was changed from host address fields to domain address fields, nothing else would be required. The exact same data structures will work for inter-domain. Only the ordering applied to the addresses must be applied to the domain numbering within the backbone fabric. The following duplicates the intermediate switch section and highlights the change required to properly work with a Fabric Domain Ordered Network.

Current US Cross Reference Classification (3):
709/220

Current US Cross Reference Classification (4):
709/238

☐ 8. Document ID: US 6247060 B1

L10: Entry 8 of 10 File: USPT Jun 12, 2001

DOCUMENT-IDENTIFIER: US 6247060 B1
TITLE: Passing a communication control block from host to a local device such that a message is processed on the device

Brief Summary Text (11):
The above description of layered protocol processing is simplified, as college-level textbooks devoted primarily to this subject are available, such as Computer Networks, Third Edition (1996) by Andrew S. Tanenbaum, which is incorporated herein by reference. As defined in that book, a computer network is an interconnected collection of autonomous computers, such as internet and intranet systems, including local area networks (LANs), wide area networks (WANs), asynchronous transfer mode (ATM), ring or token ring, wired, wireless, satellite or other means for providing communication capability between separate processors. A computer is defined herein to include a device having both logic and memory functions for processing data, while computers or hosts connected to a network are said to be heterogeneous if they function according to different operating systems or communicate via different architectures.

Detailed Description Text (99):
When a frame is received by the INIC, it must verify it completely before it even determines whether it belongs to one of its TCBs or not. This includes all header validation (is it IP, IPV4 or V6, is the IP header checksum correct, is the TCP checksum correct, etc). Once this is done it must compare the source and destination IP address and the source and destination TCP port with those in each of its TCBs to determine if it is associated with one of its TCBs. This is an expensive process. To expedite this, we have added several features in hardware to assist us. The header is fully parsed by hardware and its type is summarized in a single status word. The checksum is also verified automatically in hardware, and a hash key is created out of the IP addresses and TCP ports to expedite TCB lookup. For full details on these and other hardware optimizations, refer to the INIC Hardware Specification sections (Heading 8).

Detailed Description Text (808):

The Map instruction is provided to allow replacement of instructions which have been stored in ROM and is implemented any time the "map enable" (MapEn) bit has been set and the content of the "map address" (MapAddr) field is non-zero. The instruction decoder forces a jump instruction with the Alu operation and destination fields set to pass the MapAddr field to the program control block.

Current US Original Classification (1):
709/238

Current US Cross Reference Classification (1):
709/230

☐ 9. Document ID: US 6070187 A

L10: Entry 9 of 10 File: USPT May 30, 2000

DOCUMENT-IDENTIFIER: US 6070187 A
TITLE: Method and apparatus for configuring a network node to be its own gateway

Abstract Text (1):
A configuration agent allows a network node seeking to be automatically configured with an IP address and a default gateway address to be configured as its own gateway. In first and second embodiments of the present invention, the configuration agent resides on a network device (such as a switch or bridge) that is coupled to two network segments, with one network segments including a node to be configured and another network segment including a server capable of automatically providing configuration parameters. In the first embodiment, the configuration agent acts as a snoopy agent. Messages from the configuration server to the node to be configured are "snooped" to discover messages containing an IP address and a default gateway address. Such messages are altered to copy the IP addresses offered to the nodes seeking configuration to the default gateway addresses, and the messages are sent on their way, thereby causing the node seeking to be configured to be its own default gateway. In the second embodiment of the invention, the configuration acts as a proxy agent. From the point of view of the node to be configured, the proxy agent appears to be a configuration agent. From the point of view of the configuration server, the proxy agent appears to be a relay agent if the configuration server and the node to be configured are on different subnets. When the configuration server sends messages to the node to be configured (possibly treating the proxy agent as a relay agent), the proxy agent intercepts the message and copies the offered IP address to the default gateway address in the message, thereby causing the node seeking to be configured to be configured as its own gateway. The proxy agent also substitutes its IP address for the IP address of the actual configuration server, thereby causing the node seeking to be configured to treat the proxy agent as the configuration agent.

Brief Summary Text (18):
Assume that node 28 has an IP address of 192.44.133.13, and assume that node 30 has an IP address of 192.44.133.25. Further assume that the subnet mask of node 28 is set to 255.255.255.0. To send a packet to node 30, node 28 first does a bit-wise AND of the IP address of node 30 with the subnet mask and compares the result to a bit-wise AND of the IP address of node 28 and the subnet mask. If the results of the two AND operations match, node 30 is on the same subnet as node 28 and the MAC address of node 30 may be found using the ARP. Next, node 28 sends out a broadcast Ethernet packet with its own MAC address and the IP address of node 30 in accordance with the ARP. The Ethernet protocol supports unicast and broadcast packets. A broadcast packet is addressed to and received by all nodes on a subnet, while a unicast packet is addressed to and received by a specific node. Node 30 responds to

this message by transmitting a unicast packet containing the MAC address of node 30 back to node 28. Node 28 then transmits the TCP/IP packet to node 30 using the MAC address that it just received from node 30. Furthermore, nodes cache this information for future transmissions, thereby minimizing the need to repeatedly find the MAC address of nodes on the same subnet.

Brief Summary Text (35):
When the configuration server sends messages to the node to be configured (possibly treating the proxy agent as a relay agent), the proxy agent intercepts the message and copies the offered IP address to the default gateway address in the message, thereby causing the node seeking to be configured to be configured as its own gateway. The proxy agent also substitutes its IP address for the IP address of the actual configuration server, thereby causing the node seeking to be configured to treat the proxy agent as the configuration agent.

Detailed Description Text (2):
The present invention is a configuration agent that resides on a network device, such as a switch. The configuration agent allows a network node that is seeking configuration parameters to be configured as its own default gateway for the purpose of communicating directly with nodes that are on the same subnet, even though a subnet mask may indicate that the nodes may be on different subnets. Before discussing the present invention in greater detail below, it is helpful to understand some current trends in the art of computer networking.

Detailed Description Text (4):
As discussed above, two TCP/IP nodes connected via an Ethernet network can communicate directly without a router provided that the subnet mask of a sending node indicates that the destination IP address is on the same Ethernet network. The sending node performs a bit-wise AND operation with the subnet mask and its IP address and compares the result to a bit-wise AND of the subnet mask and the destination IP address. If the results match, the sending node uses the Address Resolution Protocol (ARP) to convert the IP address to an Ethernet address before sending out a TCP/IP packet. As used her(in, the term "hardware address" will refer to a lower level address used by the networking hardware, such as an Ethernet MAC address. The term "network address" will refer to the address used at higher levels of the protocol stack, such as an IP address.

Detailed Description Text (9):
Since the ARP is used to resolve all IP addresses, all packets on the same subnet are routed by switches, and a router is only used to transmit packets that are truly off the Ethernet network. TCP/IP packets transmitted within the network are transmitted more quickly because switches are faster than routers. Compared to the subnet mask mechanism, the gateway subroutine is not limited to adding IP addresses in powers of two. Thor do added ranges have to be contiguous. Therefore, the network administrator has more flexibility in assigning IP addresses to an Ethernet network.

Current US Original Classification (1):
709/220

Current US Cross Reference Classification (1):
709/221

☐ 10. Document ID: US 5473599 A

L10: Entry 10 of 10 File: USPT Dec 5, 1995

DOCUMENT-IDENTIFIER: US 5473599 A

TITLE: Standby router protocol

Brief Summary Text (3):
Local area networks (LANs) are commonly connected with one another through one or more routers so that a host (a PC or other arbitrary LAN entity) on one LAN can communicate with other hosts on different LANs. Typically, the host recognizes only those addresses for the entities on its LAN. When it receives a request to send a data packet to an address that it does not recognize, it communicates through a router which determines how to direct the packet between the host and the address. Unfortunately, a router may, for a variety of reasons, become inoperative (e.g., a power failure, rebooting, scheduled maintenance, etc.). When this happens, the host communicating through the inoperative router may still remain connected to other LANs if it can send packets to another router connected to its LAN.

Brief Summary Text (11):
In one aspect, the present invention provides a router for use in the described standby group. Such a router includes (1) a primary router address; (2) a group virtual address which is adopted by the router when it becomes the active router of the network segment; (3) means for assuming the group's virtual address; (4) means for issuing a coup message to notify a current active router that the router will attempt to replace the active router; and (5) means for disabling the means for issuing a coup message. In preferred embodiments, each router of this invention has the capability of adopting both the standby and active statuses depending upon the current circumstances in the network.

Detailed Description Text (35):
As suggested, each router has a specified priority which is used in elections and coups of the active router. A priority is configured for each router by a user of the network. The priority of each router is preferably an integer between 0 and 255 (i.e., an 8 bit word.) with 100 being the default. Generally, the router having the highest priority should be the active router and the router having the second highest priority should be the standby router. When routers enter or leave the network group, the priority-based elections and coups of this invention smooth the transition so that the group routers can quickly and with minimal disruption assume their correct status in the system. In the event that two routers having the same priority are seeking the same status, the primary IP addresses of these routers are compared and the router having the higher IP address is given priority.

Current US Cross Reference Classification (3):
709/244

Term	Documents
DIFFERENT	1780275
DIFFERENTS	155
NETWORKS	98430
NETWORK	254768
COMMUNICAT$	0
COMMUNICAT	14
COMMUNICATABILITY	3
COMMUNICATABLE	521
COMMUNICATABLY	42
COMMUNICATAED	1
COMMUNICATAES	2
(L8 AND (COMMUNICAT$ WITH DIFFERENT WITH NETWORKS)).USPT.	10

There are more results than shown above. Click here to view the entire set.

Display Format: KWIC Change Format

Previous Page Next Page